

Theoretical Analyses of Quantum Counting against Decoherence Errors

Jun Hasegawa^{†‡} and Fumitaka Yura[‡]

[†] Department of Computer Science, Graduate School of Information Science and Technology, the University of Tokyo. 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.

[‡] ERATO Quantum Computation and Information Project, JST. Hongo White Building, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.

E-mail: hasepyon@is.s.u-tokyo.ac.jp, yura@qci.jst.go.jp

Abstract. In this paper, we analyze the quantum counting under the decoherence, which can find the number of solutions satisfying a given oracle. We investigate probability distributions related to the first order term of the error rate on the quantum counting with the depolarizing channel. We also implement two circuits for the quantum counting – the *ascending-order* circuit and the *descending-order* circuit – by reversing ordering of application of controlled-Grover operations. By theoretical and numerical calculations for probability distributions, we reveal the difference of probability distributions on two circuits in the presence of decoherence and show that the ascending-order circuit is more robust against the decoherence than the descending-order circuit. This property of the robustness is applicable to the phase estimation such as the factoring.

1. Introduction

Since Grover demonstrated the database search algorithm [6], many applications of this algorithm have been studied [5, 7]. The *quantum counting* [4] is one of the most important applications with using the quantum Fourier transform. Given a quantum oracle, the quantum counting can find the number t of solutions of the oracle through in N elements with $O(\sqrt{tN})$ operations, whereas $O(N)$ operations are required on a classical computer. The quantum counting is considered to be used for **NP**-complete problems because the quantum counting helps us determine the existence of a solution of these problems quadratically faster than a classical algorithm, solving whether the number of solutions is zero or non-zero. Recently, there have been works for numerical integrals based on the quantum counting, called quantum summation [1, 17, 8]. One can estimate the value of integrals with $O(1/\varepsilon)$ operations for the desired accuracy ε , while $O(1/\varepsilon^2)$ operations are needed by classical Monte Carlo method.

When we realize such quantum algorithms, decoherence is inevitable since our apparatus are surrounded with environment and open systems for us. Therefore treating the decoherence should be always one of significant problems. In the previous works, there have been only a few analyses of the decoherence, related to especially Shor's factoring [15] and Grover's database search algorithm. Azuma [2] investigated the decoherence on Grover's algorithm by calculating quantum states in detail up to the fifth order term of the decoherence for σ_z errors. Shapira et al. [14] dealt with the decoherence on Grover's algorithm by changing the Hadamard transformation into some distorted operation. Yu et al. [18] represented disturbed unitary operations by the decoherence by focusing on quantum Hamiltonian and analyzed the evolution of quantum system on Grover's database search algorithm. Sun et al. [16] showed effects of environment based on the dynamic approach for quantum measurement through the example of the factoring. Several researchers have been investigated the decoherence by numerical calculations. Obenland et al. [12] simulated the circuits which factored the numbers 15, 21, 35, and 57 as well as circuits that solved the database search for a trapped ion quantum computer. Niwa et al. implemented the general-purpose parallel simulator for quantum computing which could simulate not only the factoring and the database search algorithm [10] but also quantum error correcting codes [11], and revealed influences of the decoherence and another quantum error – operational error – to these algorithms. Although the decoherence on the factoring and the database search have been analyzed in a variety of ways, there have been no analysis of the decoherence on the quantum counting.

In this paper, we investigate the decoherence related to the first order term of error rate on the quantum counting and expand our results to the phase estimation algorithm such as the factoring. The quantum counting is composed of two registers, called the *first register* and the *second register*. We assume the depolarizing channel as error models and calculate probability distributions on the quantum counting in two cases that the decoherence error occurs on each register.

We have another purpose in this paper to reveal which implementation for the quantum counting and one of the key quantum algorithms, the *phase estimation*, is robust against decoherence. Two quantum algorithms estimate a phase of a unitary operator by using the quantum Fourier transform and can be implemented in many ways by changing ordering of application of the unitary operations. In order to show the difference of effects of decoherence among different implementations, we implement two typical circuits – the *ascending-order* circuit and the *descending-order* circuit and compare probability distributions on these circuits in the presence of decoherence.

In the case that the depolarizing channel is applied on the first register in the quantum counting, we show that a probability distribution has many peaks caused by the decoherence at a distance of the power of two from correct peaks. We also show that probability distributions between the ascending-order and the descending-order circuit are the same. On the other hand, in the case of the second register, we reveal probability distributions on two circuits are completely different. In the ascending-order case, wrong outputs near correct one are obtained by the quantum counting, while in the descending-order case, two wrong outputs 0 and N are obtained with high probability independently of an input oracle. Additionally, the correct output is obtained with higher probability on the ascending-order circuit than on the descending-order one. It follows that the ascending-order implementation for the quantum counting is more robust against the decoherence.

We also show robustness against decoherence on the phase estimation with the ascending-order. Finally, we discuss weakness against decoherence on an efficient implementation for the phase estimation and the quantum counting, called the *semi-classical* implementation [13].

The rest of this paper is organized as follows: In Section 2, we begin by explaining the quantum counting and the depolarizing channel used in this paper, and implementing two quantum counting circuits. In Section 3, we analyze the decoherence on the quantum counting. We first consider analysis model for the decoherence, and then investigate probability distributions on the quantum counting in the presence of the decoherence on the first register and the second register. In Section 4, we also discuss influences of decoherence on the phase estimation and on the semi-classical implementation. In Section 5, we summarize our results. Finally, we give some detailed calculations of probability distributions in the case that the decoherence error occurs on the first register and the second one in Appendix A and Appendix B, respectively.

2. Definitions, notations, and decoherence model

First of all, we describe definitions and notations of the quantum counting used in this paper, and explain our decoherence model. We also implement two quantum counting circuits for revealing robustness against decoherence.

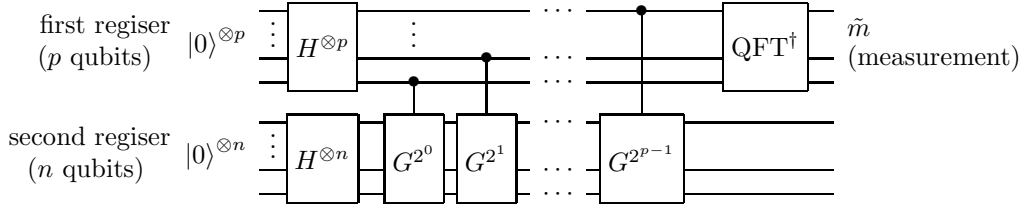


Figure 1. Circuit for the quantum counting

2.1. Quantum counting

Suppose that there are unordered $N := 2^n$ elements and a function $f : \{0, \dots, N-1\} \rightarrow \{0, 1\}$ is given as an *oracle* (a black box). Let \mathcal{I} be a set of elements which satisfy $f(x) = 1$ of N elements, that is,

$$f(x) = \begin{cases} 1 & (x \in \mathcal{I}) \\ 0 & (x \notin \mathcal{I}) \end{cases},$$

and $t := |\mathcal{I}|$. The goal of a quantum counting algorithm is to estimate the number t of solutions of the oracle f [4].

In order to estimate t , the quantum counting estimates the phase of a unitary operator G , called *Grover operator*, by using the quantum Fourier transform. Let $|x\rangle \in \mathcal{H} := (\mathbb{C}^2)^{\otimes n}$, where $(0 \leq x \leq 2^n - 1)$ be quantum states which represent 2^n elements. Grover operator G is defined as $G := U_2 U_1$ on \mathcal{H} , where $U_1 := \sum_x (-1)^{f(x)} |x\rangle\langle x|$, $U_2 := 2|s\rangle\langle s| - \mathbf{1}_N$, $|s\rangle := \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$. The operator G can be rewritten as a rotation on two-dimensional space. We divide the Hilbert space \mathcal{H} into the “good” space $\mathcal{H}_g := \text{span}_{x \in \mathcal{I}} \{|x\rangle\}$ and the “bad” space $\mathcal{H}_b := \text{span}_{x \notin \mathcal{I}} \{|x\rangle\}$ and define two orthonormal states on each space:

$$\begin{aligned} |b\rangle &:= \frac{1}{\sqrt{N-t}} \sum_{x \notin \mathcal{I}} |x\rangle \in \mathcal{H}_b, \\ |g\rangle &:= \frac{1}{\sqrt{t}} \sum_{x \in \mathcal{I}} |x\rangle \in \mathcal{H}_g. \end{aligned} \tag{1}$$

The two-dimensional vector space spanned by the bases $|b\rangle$ and $|g\rangle$ is called *Grover space*. The Grover operator G can be represented on the Grover space as follows:

$$G \equiv \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \tag{2}$$

where $\sin(\theta/2) := \sqrt{t/N}$.

Figure 1 shows a circuit for the quantum counting. We refer to the upper p qubits in this figure as a *first register* and the lower n qubits as a *second register*. The quantum counting algorithm is composed of the following five stages.

- (i) Prepare an initial state $|0\rangle^{\otimes(p+n)}$.

- (ii) Apply the Hadamard transformation H to all qubits: $\frac{1}{\sqrt{P}} \sum_{m=0}^{P-1} |m\rangle \otimes |s\rangle$, where $P := 2^p$, $|m\rangle$ and $|s\rangle$ belong to the first and second register, respectively.
- (iii) Apply controlled- G to the second register according to the first register $|m\rangle$.

$$\frac{1}{\sqrt{P}} \sum_{m=0}^{P-1} |m\rangle \otimes G^m |s\rangle.$$

- (iv) Apply the inverse Fourier transform to the first register.

$$\begin{aligned} & \frac{1}{P} \sum_{m'=0}^{P-1} |m'\rangle \otimes \sum_{m=0}^{P-1} \exp\left(2\pi i \frac{mm'}{P}\right) G^m |s\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{m'=0}^{P-1} e^{\frac{P-1}{P}\pi i m'} |m'\rangle \\ & \otimes \left[e^{\pi i f} \frac{\sin[\pi(m' + f)]}{P \sin[\pi(m' + f)/P]} |+\rangle + e^{-\pi i f} \frac{\sin[\pi(m' - f)]}{P \sin[\pi(m' - f)/P]} |-\rangle \right], \quad (3) \end{aligned}$$

where $f := P\theta/2\pi$, $|\pm\rangle := \frac{1}{\sqrt{2}}(|b\rangle \mp i|g\rangle)$.

- (v) Measure the first register and obtain \tilde{m} for a good estimator of f .

In order to determine the number of solutions from the measurement result \tilde{m} , we calculate $\tilde{t} := N \sin^2(\tilde{\theta}/2) = N \sin^2(\pi \tilde{m}/P)$. Since the probability distribution of Equation (3) has peaks at $\tilde{m} \simeq f, P - f$ ($P \gg 1$), we obtain the output \tilde{t} with high probability, which is an approximation of t for the quantum counting.

In this algorithm, we have to fix the parameter P that determines the precision. At first, by running this algorithm with setting P at \sqrt{N} , we obtain an approximated \tilde{t} such that $|t - \tilde{t}| < 2\pi\sqrt{\tilde{t}} + \pi^2$. Then, by running it again with setting P at $20\sqrt{\tilde{t}N}$, we obtain *new* estimation \tilde{t} as a more precise result. It is guaranteed to obtain t with probability at least $8/\pi^2$ [4]. It follows that the time needed for the quantum counting is $O(2^p) = O(\sqrt{tN})$.

In Figure 2, we show an example of the probability distribution of $|m'\rangle$ in Equation (3) for the quantum counting, by setting $p = 6$, $n = 8$, $\mathcal{I} = \{0, \dots, 12\}$. We also show a probability distribution of the corresponding output t' in Figure 3. The probability distribution of m' has two peaks, and that of t' has single peak at t that is the desired number of solutions.

2.2. Decoherence model

In order to analyze the decoherence, we need to model decoherence error. One of useful error models on classical information is the binary symmetric channel, which flips a bit with probability p and leaves it alone with probability $1 - p$. We consider the following quantum decoherence model analogous to the binary symmetric channel, which is often used for analyzing error correcting codes.

If we do not know anything about properties of errors that the quantum system suffers from, it is one of reasonable error models that quantum states are disturbed into

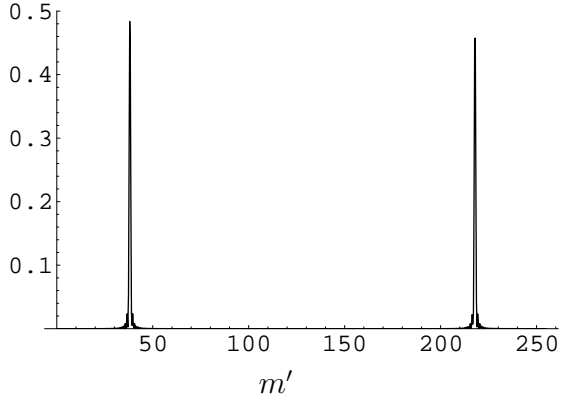


Figure 2. The probability distribution of the measurement result m' . Peaks appear near $f \simeq 38$ and $2^p - f \simeq 218$.

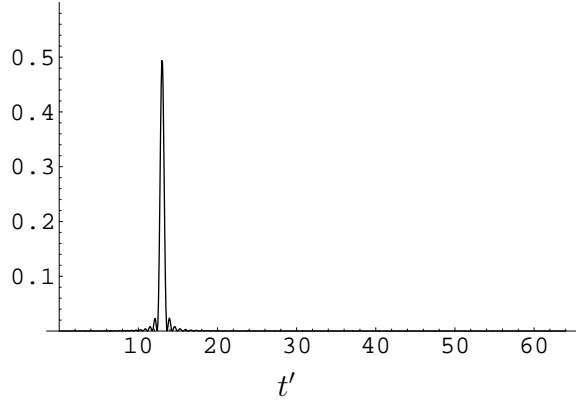


Figure 3. The probability distribution of the output t' .

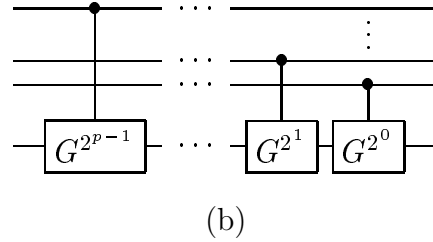
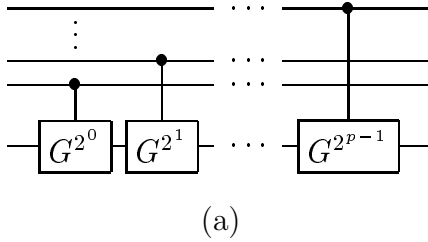


Figure 4. Two implementations of controlled- G^m operations. The ordering (a) and (b) are called the *ascending-order* and the *descending-order*, respectively. Two circuits are *equivalent* if no error occurs.

maximally mixed state as time goes on. In this paper, we assume that errors occur as local *depolarizing channel*.

Definition 1 (depolarizing channel [9]).

$$\begin{aligned} \rho &\rightarrow (1-d)\rho + d \cdot \frac{I}{2} \\ &= (1-d)\rho + d \cdot \frac{\sigma_0 \rho \sigma_0 + \sigma_x \rho \sigma_x + \sigma_y \rho \sigma_y + \sigma_z \rho \sigma_z}{4}, \end{aligned} \quad (4)$$

where ρ is a density matrix on \mathbb{C}^2 , σ_0 is the identity operator, and $\sigma_x, \sigma_y, \sigma_z$ are *Pauli* matrices.

We apply this time-discretized error to each qubit at each unit time regardless of the existence of a quantum gate on the qubit. Since Equation (4) is represented by summation of classical events, we simulate this channel by applying $\sigma_x, \sigma_y, \sigma_z$, and σ_0 to each qubit with probability $d/4$; otherwise the state is left untouched. On our numerical calculations, we take an average of experiments by using only pure states.

2.3. Two implementations for the quantum counting

Generally speaking, unitary operations in circuit are not commutative. In the quantum counting circuit, however, all controlled- G gates are commutative. Figure 4 shows examples of *equivalent* implementations for the quantum counting, i.e. probability distributions on two implementations are completely the same in no decoherence case. One of difficulties in the analysis of decoherence is that we can not exchange the operators that are commutative in the system which is affected by decoherence.

One of our aims in this paper is to reveal how different influences of the decoherence on *equivalent* circuits are and which implementation is more robust against the decoherence. In order to investigate it, we implement two typical circuits for the quantum counting.

Definition 2 (two implementations for the quantum counting). We define two quantum counting circuits with the following ordering.

ascending-order from the controlled- G^{2^0} operation in Figure 4 (a).

descending-order from the controlled- $G^{2^{p-1}}$ operations in Figure 4 (b).

The descending-order implementation is especially needed for an efficient implementation of the quantum counting and the phase estimation algorithm, which reduces the number of qubits on the first register to one. We discuss these efficient implementations in Section 4.2 later.

3. Decoherence on the quantum counting

In this section, we analyze influences of the decoherence on the quantum counting. We begin by explaining our analysis model and then investigate the decoherence on the first and the second register in two quantum counting circuits with the ascending-order and the descending-order. Finally, we discuss the robust implementation for the quantum counting against the decoherence.

3.1. Analysis model for the decoherence

The probability that the decoherence error occurs is considered to increase in proportion to the product of execution time and the number of qubits. As stated in Section 2.1, the quantum counting is performed in five stages: (i) preparing an initial state, (ii) applying the Hadamard transformation, (iii) applying controlled- G operations, (iv) applying the inverse quantum Fourier transform, and (v) measurements. The time needed for each stage is as follows: The stage (i) and (v) are considered to be one step. Application of the Hadamard transformations on the stage (ii) takes $O(1)$ and application of the inverse quantum Fourier transform on the stage (iv) takes at most $O(p^2)$. In contrast, application of controlled- G operations on the stage (iii) takes $2^p - 1$, which is exponential to p . It follows that the decoherence error happens on the stage (iii) with exponentially

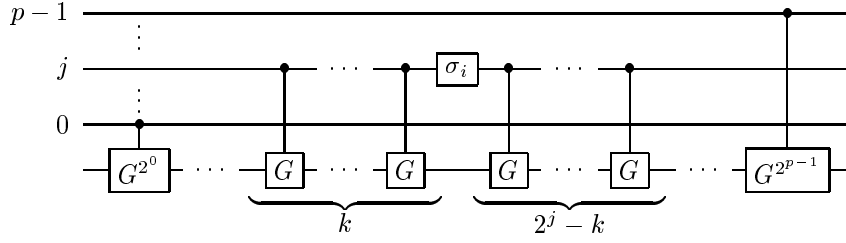


Figure 5. σ_i error occurs on the j -th qubit of the first register after application of controlled- G^k operations with the j -th control qubit.

higher probability than on other stages. On our analyses, we restrict the position of the error only on the stage (iii).

Suppose that the error rate d is small enough ($d \ll 1$), then influences of the decoherence are approximated by the first order term of d . This means that the depolarizing channel is applied only once. Since the quantum counting has two registers, the register where the depolarizing channel is applied is either of the first register or the second one.

Under these conditions, we calculate probability distributions on the quantum counting, and give some properties of the decoherence on two registers. Moreover, we compare influences of the decoherence on the ascending-order and the descending-order implementations.

3.2. Decoherence on the first register

We analyze the decoherence on the first register by considering the case that the error based on the depolarizing channel occurs once on the first register. Through the depolarizing channel, $\sigma_x, \sigma_y, \sigma_z$ errors and identity operator σ_0 occur with the same rate from Equation (4). We first deal with the ascending-order circuit in Figure 4 (a).

We investigate influences of the decoherence by calculating probability distributions on the quantum counting. For calculations, we need to represent the position of σ_i error. As stated above, we already restrict the position of the decoherence on the state (iii). Let j and k be integers such that the error occurs

- on the j -th qubit of the first register,
- after application of controlled- G^k operations with the j -th control qubit,

where $0 \leq j \leq p-1$, $0 \leq k \leq 2^j$. These parameters are sufficient for determining where and when σ_i error occurs. The case that the error occurs on the j -th qubit before(after) controlled- G^{2^j} can be represented by $k = 0(k = 2^j)$ respectively since our decoherence model is local. Figure 5 shows the position of σ_i error on our analyses. The total number of applications of controlled- G operations before the error is $2^j + k - 1$.

We first focus on the position of peaks in a probability distribution on the quantum counting under the decoherence. If no error occurs, the probability distribution has only

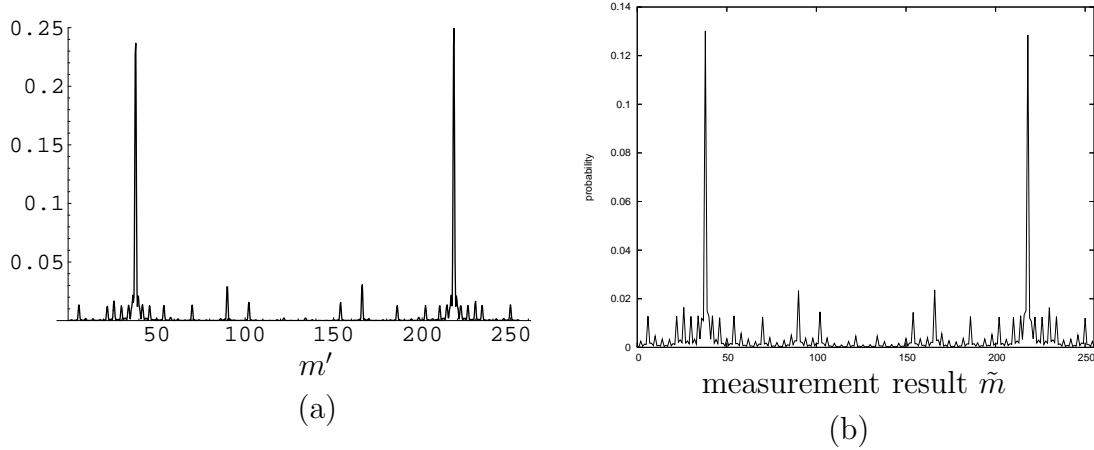


Figure 6. The probability distributions of measurement results with the same parameters in Figure 2. (a): $\frac{1}{4p} \sum_{j=0}^{p-1} \sum_{i=0,x,y,z} \text{Prob}^{(i,j,k)}(m')$. (b): the average of numerical calculations 10^5 trials where the error rate $d = 4 \times 10^{-3}$.

two correct peaks near $\tilde{m} \simeq f, 2^p - f$, as shown in Equation (3). Let $\text{Prob}^{(i,j,k)}(m')$ be the probability to obtain m' as a measurement result in the case of the above position of σ_i error. By calculation $\text{Prob}^{(i,j,k)}(m')$ in Appendix A, we have

$$\begin{aligned} \sum_{i=0,x,y,z} \text{Prob}^{(i,j,k)}(m') = & \left[\frac{\sin \{\pi(m' + f)\}}{2^{p-j-1} \sin \{\pi/2^{p-j-1}(m' + f)\}} \times \frac{2^{p-j} \sin \{\pi/2^{p-j}(m' + f)\}}{2^p \sin \{\pi/2^p(m' + f)\}} \right]^2 \\ & + \left[\frac{\sin \pi(m' - f)}{2^{p-j-1} \sin \{\pi/2^{p-j-1}(m' - f)\}} \times \frac{2^{p-j} \sin \{\pi/2^{p-j}(m' - f)\}}{2^p \sin \{\pi/2^p(m' - f)\}} \right]^2. \end{aligned} \quad (5)$$

This equation has two strong peaks at $m' \simeq f, -f \equiv 2^p - f$ that are the same as the correct peaks and weak peaks at a distance of $\pm 2^{p-j-1}$ from the strong peaks, which is caused by errors.

Proposition 1. *The probability distribution related to the first order term of the error rate on the quantum counting mainly has wrong peaks at a distance of the power of two from $\tilde{m} \simeq f, 2^p - f$ if the depolarizing channel is applied on the first register.*

We show the graph of $\frac{1}{4p} \sum_{i=0,x,y,z} \sum_{j=0}^{p-1} \text{Prob}^{(i,j,k)}(m')$ in Figure 6 (a), which means the average of probability distributions in all error cases. We also show the graph of numerical calculations in Figure 6 (b). We did the experiments on Quantum Computation Simulation System (QCSS) [10] and took the average of 10^5 trials. On the numerical calculations, we set the error rate $d = 4 \times 10^{-3}$ so that the decoherence errors based on the depolarizing channel occur on the first register about twice on each trial.

Proposition 1 follows the number of wrong peaks caused by the decoherence.

Claim 2. *The number of main wrong peaks is $O(p)$ in probability distribution related to the first order term of the error rate if the depolarizing channel is applied on the first*

register.

The probability distribution $\sum_{i=0,x,y,z} \text{Prob}^{(i,j,k)}(m')$ does not depend on k that determines *depth* of σ_i error, i.e. the time when the error occurs.

Proposition 3. *The probability distribution related to the first order term of the error rate on the quantum counting is independent of depth of error if the depolarizing channel is applied on the first register.*

Proposition 3 means that there is no difference of influences of the decoherence between on the ascending-order circuit and on the descending-order one for the quantum counting, since controlled-Grover operators are commutative each other.

Proposition 4. *Probability distributions related to the first order term of the error rate on the quantum counting are independent of the ordering of application of controlled-G operations if the depolarizing channel is applied on the first register.*

3.3. Decoherence on the second register

We then deal with the case that the decoherence error occurs once on the second register in the quantum counting. In Section 3.2, we treat the error on the first register, which consists of control gates. In that case, error affects only the number of application m of controlled- G^m . On the other hand, the error on the second register modifies the state on which Grover operator acts. Because the states $|b\rangle$ and $|g\rangle$ depend on the quantum oracle, we can not specify how the second register is disturbed by the decoherence. We need to consider the disturbance and action of Grover operator on a disturbed second register.

We first show action of Grover operator on an arbitrary quantum state in order to deal with the operator on a disturbed second register. Any quantum state $|\phi\rangle \in \mathcal{H}$ is decomposed as follows by means of Gram-Schmidt orthogonalization:

$$|\phi\rangle := u^{(\phi)} |b\rangle + v^{(\phi)} |g\rangle + u_e^{(\phi)} |e_b^{(\phi)}\rangle + v_e^{(\phi)} |e_g^{(\phi)}\rangle, \quad (6)$$

where $u^{(\phi)}, v^{(\phi)}, u_e^{(\phi)}, v_e^{(\phi)} \in \mathbb{C}$, $|e_b^{(\phi)}\rangle \in \mathcal{H}_b$, $|e_g^{(\phi)}\rangle \in \mathcal{H}_g$, and $|e_b^{(\phi)}\rangle$ and $|e_g^{(\phi)}\rangle$ are determined such that $\langle b|e_b^{(\phi)}\rangle = \langle g|e_g^{(\phi)}\rangle = 0$. By definition of Grover operator, we obtain the following lemma.

Lemma 5. *For any quantum state $|\phi\rangle$, Grover operator G can be rewritten as:*

$$G \equiv \begin{pmatrix} \cos \theta & -\sin \theta & 0 & 0 \\ \sin \theta & \cos \theta & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (7)$$

on four-dimensional space spanned by the basis states $|b\rangle, |g\rangle, |e_b^{(\phi)}\rangle$, and $|e_g^{(\phi)}\rangle$, which satisfy $|e_b^{(\phi)}\rangle \in \mathcal{H}_b$, $|e_g^{(\phi)}\rangle \in \mathcal{H}_g$, $\langle b|e_b^{(\phi)}\rangle = \langle g|e_g^{(\phi)}\rangle = 0$.

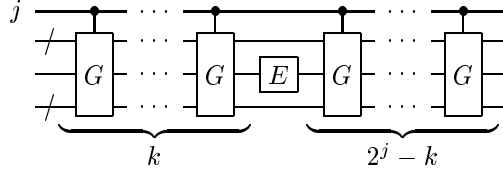


Figure 7. Some error E occurs on the second register after application of controlled- G^k operations with the j -th control qubit ($0 \leq j \leq p-1, 0 \leq k \leq 2^j$).

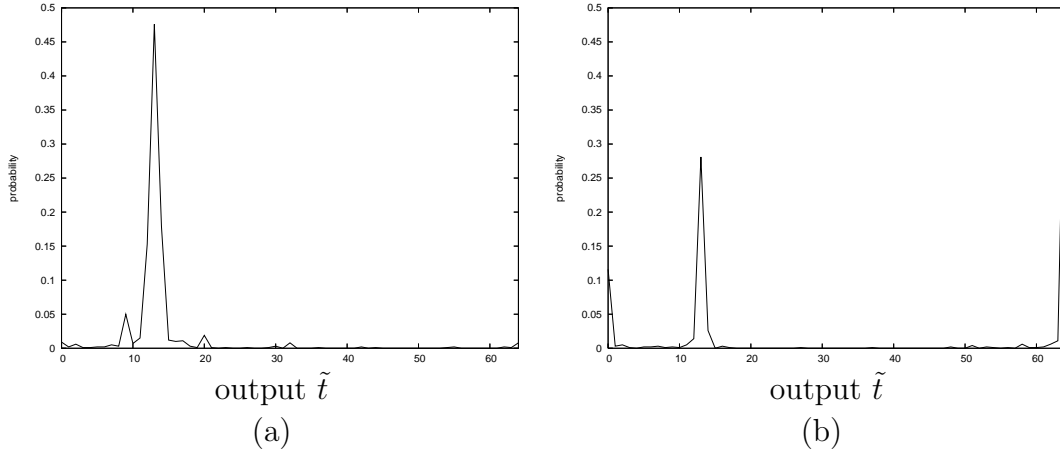


Figure 8. The probability distributions of the output \tilde{t} by numerical calculations 10^3 trials with the error rate $d = 4 \times 10^{-3}$. (a): on the ascending-order circuit, (b): on the descending-order circuit.

Before disturbance, the second register is a superposition of the states $|b\rangle$ and $|g\rangle$. If some error occurs on the register, two states are disturbed into

$$\begin{aligned} |b\rangle &\rightarrow u^{(b)} |b\rangle + v^{(b)} |g\rangle + u_e^{(b)} |e_b^{(b)}\rangle + v_e^{(b)} |e_g^{(b)}\rangle, \\ |g\rangle &\rightarrow u^{(g)} |b\rangle + v^{(g)} |g\rangle + u_e^{(g)} |e_b^{(g)}\rangle + v_e^{(g)} |e_g^{(g)}\rangle, \end{aligned} \quad (8)$$

satisfying

$$\begin{aligned} |e_b^{(b)}\rangle, |e_b^{(g)}\rangle &\in \mathcal{H}_b, \quad |e_g^{(b)}\rangle, |e_g^{(g)}\rangle \in \mathcal{H}_g, \\ \langle b|e_b^{(b)}\rangle &= \langle b|e_b^{(g)}\rangle = \langle g|e_g^{(b)}\rangle = \langle g|e_g^{(g)}\rangle = 0. \end{aligned} \quad (9)$$

Lemma 6. Any disturbed second register by the decoherence can be represented by the superpositions of $|b\rangle, |g\rangle, |e_b^{(b)}\rangle, |e_b^{(g)}\rangle, |e_g^{(b)}\rangle$, and $|e_g^{(g)}\rangle$, satisfying Equation (9). Action of Grover operator is a rotation by θ on two-dimensional space spanned by $|b\rangle$ and $|g\rangle$, by π on $|e_b^{(b)}\rangle$ and $|e_b^{(g)}\rangle$, and by 0 on $|e_g^{(b)}\rangle$ and $|e_g^{(g)}\rangle$.

Like the case of the first register, we consider that some error E , not necessarily the depolarizing channel, is applied on the second register after application of controlled- G^k operations with the j -th control qubit, as shown in Figure 7. In this case, a probability distribution before measurement on the ascending-order circuit has peaks near $m' \simeq f, 2^p - f$ that are the same as ones in no error case, as detailed in Appendix

B. On the other hand, a probability distribution on the descending-order circuit has peaks not only near $m' \simeq f, 2^p - f$ but also at $m' = 0, 2^p/2$ with high probability, independently of the quantum oracle. By calculating an output $t' = N \sin^2(\pi m'/2^p)$ of the quantum counting, we obtain the following proposition.

Proposition 7. *The following wrong outputs of the quantum counting related to the first order term of the error rate are obtained with high probability if some decoherence error occurs on the second register:*

- *Wrong outputs near t in the ascending-order case.*
- *Wrong outputs 0 and N in the descending-order case, independently of the quantum oracle.*

We show two graphs of outputs of the quantum counting with the ascending-order and the descending-order by numerical calculations in Figure 8 (a) and (b), respectively. These experiments were done 10^3 trials with the same conditions as the first register case except that the decoherence error occurs on the second register.

The difference of positions of wrong peaks between two quantum counting circuits can be intuitively considered as follows: If a decoherence error occurs on the second register, influences of the error propagate to the first register by controlled- G operators. On the ascending-order circuit, G s are applied from the controlled- G^{2^0} with the 0th control qubit corresponding to the MSB of a measurement result. The influences therefore propagate the 0th control qubit(MSB) to $(p - 1)$ th control qubit(LSB). Since application of controlled- G^m operations with the LSB needs more time exponentially than with the MSB, decoherence error occurs with exponential higher probability on controlled- G^m operations with low control qubits. It follows that influences of the error propagate to only low control qubits. On the other hand, in the descending-order case, the influences propagate from the LSB to the MSB of the first register because of reversed ordering of application of controlled- G operations. Therefore not only low control qubits but also high qubits are affected by the decoherence.

We finally consider the probability to obtain the correct output for the quantum counting. Peaks in the probability distribution on the descending-order circuit are distributed to four peaks whereas the probability distribution on the ascending-order circuit has only the correct two peaks.

Proposition 8. *The correct output of the quantum counting is obtained with higher probability on the ascending-order circuit than on the descending-order circuit if the decoherence error occurs on the second register.*

3.4. Robust implementation against the decoherence

Proposition 4 shows that the probability to obtain the correct output on the ascending-order is the same as the probability on the descending-order one in the case of decoherence on the first register. Proposition 8 together with the proposition states the following robustness against the decoherence on two registers in the quantum counting.

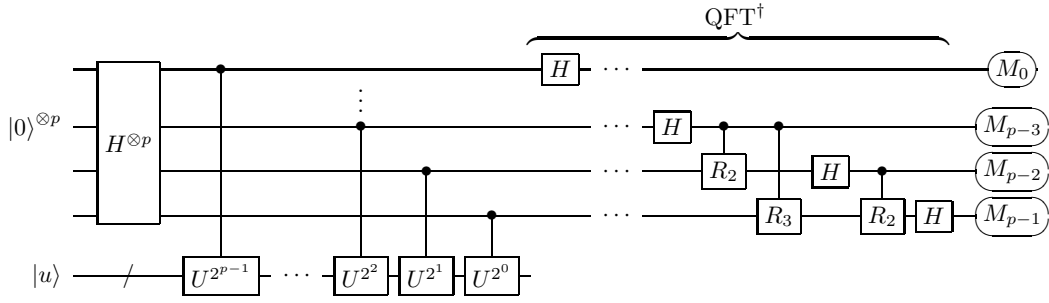


Figure 9. Circuit for the phase estimation with the descending-order. Controlled rotations R_j are defined as $R_j := \begin{pmatrix} 1 & 0 \\ 0 & \phi_j \end{pmatrix}$ with $\phi_j := e^{-2\pi i/2^j}$.

Claim 9. *The ascending-order implementation for the quantum counting is more robust against the decoherence than the descending-order implementation.*

4. Discussion on phase estimation algorithms

In this section, we extend our results with respect to robust implementation against the decoherence to the phase estimation. We also discuss robustness of semi-classical implementation against the decoherence.

4.1. Decoherence on phase estimation algorithms

Phase estimation is one of key quantum algorithms, used in Shor's factoring [15]. Suppose that a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$, where the value of φ is unknown. The goal of the phase estimation is to find the phase φ . A circuit for the phase estimation is shown in Figure 9. The phase estimation is performed by application of controlled- U operations to the second register prepared to the corresponding eigenvector $|u\rangle$ initially. Like the quantum counting, the phase estimation has such *equivalent* implementations as the ascending-order circuit and the descending-order circuit, by changing ordering of application of controlled- U operations instead of controlled- G operations in the quantum counting.

Claim 10. *The phase estimation can find the desired phase on the ascending-order circuit with higher probability than on the descending-order one in the presence of decoherence on the second register.*

As mentioned in Subsection 3.3, influences of the decoherence error on the second register in the quantum counting propagate only to lower qubits of the first register with exponentially high probability on the ascending-order circuit, whereas these influences propagate to higher qubits of the first register on the descending-order circuit. This propagation of decoherence is applicable not only to the quantum counting but also to the phase estimation, though positions of wrong peaks caused by the decoherence are determined by a unitary operator U on the phase estimation.

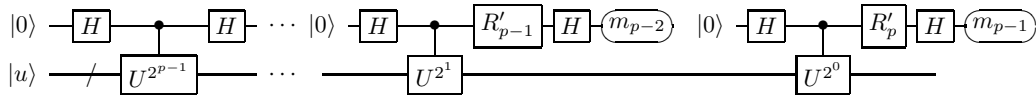


Figure 10. Semi-classical circuit for the phase estimation. R'_j is defined with the results of previous measurements: $R'_j = \begin{pmatrix} 1 & 0 \\ 0 & \phi'_j \end{pmatrix}$ with $\phi'_j := e^{-2\pi i \sum_{k=2}^j m_{j-k}/2^k}$.

4.2. Decoherence on efficient implementations for the phase estimation

An efficient implementation for the phase estimation, called the *semi-classical* implementation, was demonstrated by Parker et al. [13]. We show the semi-classical circuit for the phase estimation in Figure 10, corresponding to the circuit in Figure 9. On this circuit, inverse quantum Fourier transform and measurements are applied as fast as possible so that only single qubit is required for the first register. By using semi-classical technique, Beauregard [3] reduced the number of qubits for the factoring about half as implementations in Figure 9. It sounds so good for quantum computation since handling many qubits is considered to be difficult.

Here we discuss robustness of the semi-classical implementation against the decoherence. This implementation saves the number of qubits dramatically, although depth of circuits is almost the same as usual implementation. Since influences of the decoherence is considered to increase in proportion to product of the depth of circuits and the number of qubits, the semi-classical implementation is more robust against the decoherence from this point of view.

We next focus on the ordering of application of controlled- U operations. On the semi-classical circuit, controlled- U operations must be applied from controlled- $U^{2^{p-1}}$ operations just as the descending-order case so that measurements are done as fast as possible. Since the semi-classical implementation has single qubit for the first register, most influences of the decoherence are caused by the second register. It means that the semi-classical circuit is less robust against the decoherence like the descending-order.

We finally note the robustness of the semi-classical implementation for the quantum counting especially in order to solve **NP**-complete problems. Checking whether the number of solutions for these problems is zero or non-zero by the quantum counting helps us solve the problems. As we have shown in Proposition 7, the descending-order circuit has wrong peaks at 0 or N independently of oracle. Since the semi-classical circuit is restricted to descending-order, it may not be suitable for such problems.

5. Concluding remarks

In this paper, we focused on investigating influences of the decoherence related to the first order term of error rate on the quantum counting and revealing the difference of robustness against decoherence on two *equivalent* implementations.

In the analysis of decoherence on the first register, we showed that probability

distribution on the quantum counting had wrong peaks caused by the depolarizing channel at a distance of the power of two from correct peaks, and the probability distribution was independent of ordering of application of controlled- G operations. In the analysis on the second register, we first showed that wrong outputs were obtained near the correct one on the ascending-order circuit, whereas particular wrong outputs 0 and N were obtained with high probability on the descending-order circuit. We then clarified that the correct output were obtained with higher probability on the ascending-order circuit than on the descending-order one. Consequently, the ascending-order implementation of the quantum counting was more robust against the decoherence.

We also discussed the decoherence on the phase estimation. Similar to the quantum counting, the probability to estimate the desired phase by the phase estimation such as the factoring was higher on the ascending-order circuit. Moreover, we pointed out weakness of the semi-classical implementation against the decoherence because of the descending-order.

Acknowledgments

We are very grateful to Prof. Hiroshi Imai for giving helpful advice to us, and also thank Dr. Jumpei Niwa for providing Quantum Computation Simulation System (QCSS) for numerical calculations to us.

Appendix A. Probability distribution in the first register case

We consider the case that the decoherence error based on the depolarizing channel occurs once on the first register. Suppose that the error occurs on the j -th qubit of the first register after application of controlled- G^k with the j -th control qubit, as shown in Figure 5. Under the depolarizing channel, $\sigma_x, \sigma_y, \sigma_z$ errors disturb each qubit with the same probability. We calculate probability distributions in each error case and take an average of probability distributions of all cases for simulating the depolarizing channel with pure states.

Appendix A.1. $\sigma_x, \sigma_y, \sigma_z$ errors and identity σ_0

We first deal with σ_x error. Let $\sum_{j=0}^{P-1} m_j 2^j := m$ be indexes of the first register in the quantum counting. The quantum state before σ_x error is represented as follows:

$$\frac{1}{\sqrt{P}} \sum_{m=0}^{P-1} |m\rangle \otimes G^{km_j + (m \bmod 2^j)} |s\rangle.$$

Since σ_x error flips a bit m_j of the quantum state $|m\rangle$, the state is disturbed by σ_x into:

$$\frac{1}{\sqrt{P}} \sum_{m=0}^{P-1} |m + (1 - 2m_j)2^j\rangle \otimes G^{km_j + (m \bmod 2^j)} |s\rangle.$$

The rest of controlled- G operations and the QFT are applied to this state,

$$\begin{aligned} & \frac{1}{\sqrt{P}} \sum_{m=0}^{P-1} |m + (1 - 2m_j)2^j\rangle \otimes G^{m+(1-2m_j)(2^j-k)} |s\rangle \\ & \xrightarrow{F.T.} \sum_{m'=0}^{P-1} |m'\rangle \otimes \sum_{m=0}^{P-1} \sum_{l=\pm} c_x^{(l)} |l\rangle, \end{aligned}$$

where $|\pm\rangle := \frac{1}{\sqrt{2}}(|b\rangle \mp i|g\rangle)$ and $c_x^{(\pm)} := \frac{1}{\sqrt{2P}} e^{2\pi i \frac{mm'}{P}} e^{\pm i\theta/2} e^{\pm i\theta(m-(1-2m_j)k)}$.

By calculation of $|c_x^{(\pm)}|$, we have

$$\begin{aligned} |c_x^{(\pm)}| &= \left| \frac{1}{\sqrt{2P}} \sum_{m=0}^{P-1} \left[e^{2\pi i \frac{mm'}{P}} e^{\pm i\theta(m-(1-2m_j)k)} \right] \right| \\ &= \frac{1}{\sqrt{2}} \cdot \frac{\sin[\pi(m' \pm f)]}{2^{p-j-1} \sin[\pi(m' \pm f)/2^{p-j-1}]} \times \cos \left[\pi \left(m' \pm f \pm 2k \frac{f}{2^j} \right) / 2^{p-j} \right] \\ &\quad \times \frac{2^{p-j} \sin[\pi(m' \pm f)/2^{p-j}]}{2^p \sin[\pi(m' \pm f)/2^p]}. \end{aligned} \quad (A.1)$$

Similarly, we calculate $|c_i^{(\pm)}|$ where $i = y, z$, corresponding to σ_i errors.

$$\begin{aligned} |c_y^{(\pm)}| &= \frac{1}{\sqrt{2}} \cdot \frac{\sin[\pi(m' \pm f)]}{2^{p-j-1} \sin[\pi(m' \pm f)/2^{p-j-1}]} \times \sin \left[\pi \left(m' \pm f \pm 2k \frac{f}{2^j} \right) / 2^{p-j} \right] \\ &\quad \times \frac{2^{p-j} \sin[\pi(m' \pm f)/2^{p-j}]}{2^p \sin[\pi(m' \pm f)/2^p]}. \end{aligned} \quad (A.2)$$

$$\begin{aligned} |c_z^{(\pm)}| &= \frac{1}{\sqrt{2}} \cdot \frac{\sin[\pi(m' \pm f)]}{2^{p-j-1} \sin[\pi(m' \pm f)/2^{p-j-1}]} \times \cos [\pi(m' \pm f)/2^{p-j}] \\ &\quad \times \frac{2^{p-j} \sin[\pi(m' \pm f)/2^{p-j}]}{2^p \sin[\pi(m' \pm f)/2^p]}. \end{aligned} \quad (A.3)$$

We also calculate $|c_0^{(\pm)}|$ for symmetry of the depolarizing channel in Equation (4).

$$\begin{aligned} |c_0^{(\pm)}| &= \frac{1}{\sqrt{2}} \cdot \frac{\sin[\pi(m' + f)]}{2^p \sin[\pi(m' + f)/2^p]} \\ &= \frac{1}{\sqrt{2}} \cdot \frac{\sin[\pi(m' \pm f)]}{2^{p-j-1} \sin[\pi(m' \pm f)/2^{p-j-1}]} \times \sin [\pi(m' \pm f)/2^{p-j}] \\ &\quad \times \frac{2^{p-j} \sin[\pi(m' \pm f)/2^{p-j}]}{2^p \sin[\pi(m' \pm f)/2^p]}. \end{aligned} \quad (A.4)$$

Appendix A.2. Probability distribution of all errors

Let $Prob^{(i,j,k)}$ be the probability to observe m' as a measurement result, where $i = x, y, z, 0$, $0 \leq j \leq p-1$, and $0 \leq k \leq 2^p-1$. Taking summation of probability distributions in all cases, we obtain the following probability distribution on the depolarizing channel:

$$\frac{1}{4} \sum_{i=0,x,y,z} Prob^{(i,j,k)}(m') = \frac{1}{4} \sum_{i=x,y,z,0} \sum_{l=\pm} |c_i^{(l)}|^2$$

$$\begin{aligned}
&= \frac{1}{4} \left[\frac{\sin[\pi(m' + f)]}{2^{p-j-1} \sin[\pi(m' + f)/2^{p-j-1}]} \times \frac{2^{p-j} \sin[\pi(m' + f)/2^{p-j}]}{2^p \sin[\pi(m' + f)/2^p]} \right]^2 \\
&\quad + \frac{1}{4} \left[\frac{\sin[\pi(m' - f)]}{2^{p-j-1} \sin[\pi(m' - f)/2^{p-j-1}]} \times \frac{2^{p-j} \sin[\pi(m' - f)/2^{p-j}]}{2^p \sin[\pi(m' - f)/2^p]} \right]^2. \quad (\text{A.5})
\end{aligned}$$

$\frac{1}{4} \sum_{i=0,x,y,z} \text{Prob}^{(i,j,k)}(m')$ does not depend on k . It means that this probability distribution is uniquely determined by the qubit where the error occurs, independently of when the error occurs.

Appendix B. Probability distribution in the second register case

Here we consider to calculate probability distributions of the quantum counting when the decoherence occurs on the second register. We deal with two probability distributions on the ascending-order circuit and the descending-order one.

Appendix B.1. The ascending-order circuit

We first consider the ascending-order circuit for the quantum counting. Suppose that the decoherence error occurs on the second register after application of controlled- G^k operations with the j -th control qubit, similar to the case of first register.

Let r be the number of application of controlled- G operations according to the first register $|m\rangle$ before the decoherence occurs.

$$r := km_j + (m \bmod 2^j).$$

The quantum state in the quantum counting before the decoherence is represented as follows:

$$\frac{1}{\sqrt{P}} \sum_{m=0}^{P-1} |m\rangle \otimes \left[\cos\left(r + \frac{1}{2}\right) \theta |b\rangle + \sin\left(r + \frac{1}{2}\right) \theta |g\rangle \right].$$

By Lemma 6, the decoherence disturbs the state into

$$\frac{1}{\sqrt{P}} \sum_{m=0}^{P-1} |m\rangle \otimes \left[\cos\left(r + \frac{1}{2}\right) \theta |b'\rangle + \sin\left(r + \frac{1}{2}\right) \theta |g'\rangle \right], \quad (\text{B.1})$$

where

$$\begin{aligned}
|b'\rangle &:= u^{(b)} |b\rangle + v^{(b)} |g\rangle + u_e^{(b)} |e_b^{(b)}\rangle + v_e^{(b)} |e_g^{(b)}\rangle, \\
|g'\rangle &:= u^{(g)} |b\rangle + v^{(g)} |g\rangle + u_e^{(g)} |e_b^{(g)}\rangle + v_e^{(g)} |e_g^{(g)}\rangle,
\end{aligned}$$

satisfying Equation (9). By application of the rest of controlled- G operations and the QFT,

$$\begin{aligned}
&\frac{1}{P} \sum_{m'=0}^{P-1} \sum_{m=0}^{P-1} e^{2\pi i \frac{mm'}{P}} |m'\rangle \otimes \left[\cos\left(r + \frac{1}{2}\right) \theta \cdot G^{m-r} |b'\rangle + \sin\left(r + \frac{1}{2}\right) \theta \cdot G^{m-r} |g'\rangle \right] \\
&= \sum_{m'=0}^{P-1} |m'\rangle \otimes \frac{1}{2P} \sum_{m=0}^{P-1} e^{2\pi i \frac{mm'}{P}} \times
\end{aligned}$$

$$\begin{aligned}
& \left[e^{\frac{1}{2}i\theta} e^{ir\theta} \left\{ \frac{1}{\sqrt{2}} e^{i(m-r)\theta} \{ (u^{(b)} + iv^{(b)}) - i(u^{(g)} + iv^{(g)}) \} |+\rangle \right. \right. \\
& \quad + \frac{1}{\sqrt{2}} e^{-i(m-r)\theta} \{ (u^{(b)} - iv^{(b)}) - i(u^{(g)} - iv^{(g)}) \} |-\rangle \\
& \quad + e^{\pi i(m-r)} \left(u_e^{(b)} |e_b^{(b)}\rangle - i u_e^{(g)} |e_b^{(g)}\rangle \right) + \left(v_e^{(b)} |e_g^{(b)}\rangle - i v_e^{(g)} |e_g^{(g)}\rangle \right) \Big\} \\
& \quad + e^{-\frac{1}{2}i\theta} e^{-ir\theta} \left\{ \frac{1}{\sqrt{2}} e^{i(m-r)\theta} \{ (u^{(b)} + iv^{(b)}) + i(u^{(g)} + iv^{(g)}) \} |+\rangle \right. \\
& \quad + \frac{1}{\sqrt{2}} e^{-i(m-r)\theta} \{ (u^{(b)} - iv^{(b)}) + i(u^{(g)} - iv^{(g)}) \} |-\rangle \\
& \quad \left. \left. + e^{\pi i(m-r)} \left(u_e^{(b)} |e_b^{(b)}\rangle + i u_e^{(g)} |e_b^{(g)}\rangle \right) + \left(v_e^{(b)} |e_g^{(b)}\rangle + i v_e^{(g)} |e_g^{(g)}\rangle \right) \right\} \right] . \quad (\text{B.2})
\end{aligned}$$

We focus on peaks of each term in this equation.

Appendix B.1.1. Peaks of the terms $| \pm \rangle$

Except global factors, a coefficient of the term $|+\rangle$ in Equation (B.2) is as follows:

$$\begin{aligned}
& \frac{u^{(b)} + iv^{(b)} - i(u^{(g)} + iv^{(g)})}{2\sqrt{2}P} e^{\frac{\pi i f}{P}} \sum_{m=0}^{P-1} e^{\frac{2\pi i}{P} \{mm' + mf\}} \\
& + \frac{u^{(b)} + iv^{(b)} + i(u^{(g)} + iv^{(g)})}{2\sqrt{2}P} e^{-\frac{\pi i f}{P}} \sum_{m=0}^{P-1} e^{\frac{2\pi i}{P} \{mm' + (m-2r)f\}}.
\end{aligned}$$

Here we calculate only each summation instead of whole equation because we want to know where the term $|+\rangle$ have peaks. More precisely, we calculate the first summation

$$\left| \sum_{m=0}^{P-1} \exp \left[\frac{2\pi i}{P} \{m(m' + f)\} \right] \right| = \frac{\sin[\pi(m' + f)]}{2^p \sin[\pi(m' + f)/2^p]}, \quad (\text{B.3})$$

and the second summation

$$\begin{aligned}
d_{\text{asc}}^{(+)} &:= \left| \sum_{m=0}^{P-1} \exp \left[\frac{2\pi i}{P} \{mm' + (m-2r)f\} \right] \right| \\
&= \frac{\sin[\pi(m' + f)]}{2^{p-j-1} \sin[\pi(m' + f)/2^{p-j-1}]} \times \cos \left[\pi \left\{ m' + \left(1 - \frac{2k}{2^j} \right) f \right\} / 2^{p-j} \right] \\
&\quad \times \frac{2^{p-j} \sin[\pi(m' - f)/2^{p-j}]}{2^p \sin[\pi(m' - f)/2^p]}. \quad (\text{B.4})
\end{aligned}$$

The first summation has single peak at $m' = -f \equiv 2^p - f$ and the second summation has a strong peak at $m' = f$ and weak peaks near $m' = f$, as shown in Figure B1. It is easily seen that the term $|-\rangle$ also has two peaks at $m' = f, 2^p - f$ and weak peaks near $m' = 2^p - f$.

Appendix B.1.2. Peaks of the terms $|e_b^{(b)}\rangle$ and $|e_b^{(g)}\rangle$

We then consider peaks of the term $|e_b^{(b)}\rangle$ which consists of two summations except global factors:

$$\frac{1}{P} \sum_{m=0}^{P-1} e^{\frac{2\pi i}{P}\{mm' + rf + (m-r)\frac{P}{2}\}}, \quad \frac{1}{P} \sum_{m=0}^{P-1} e^{\frac{2\pi i}{P}\{mm' - rf + (m-r)\frac{P}{2}\}}, \quad (\text{B.5})$$

Since the term $|e_b^{(g)}\rangle$ also have two same summations, we describe $|e_b\rangle$ as terms $|e_b^{(b)}\rangle$ and $|e_b^{(g)}\rangle$ for calculating peaks of the terms together.

Let $d_{\text{asc}}^{(e_b)}$ be the first summation in Equation (B.5).

$$\begin{aligned} d_{\text{asc}}^{(e_b)} &:= \left| \frac{1}{P} \sum_{m=0}^{P-1} \exp \left[\frac{2\pi i}{P} \left\{ mm' + rf + (m-r)\frac{P}{2} \right\} \right] \right| \\ &\equiv \frac{\sin[\pi(m' + \frac{P}{2})]}{2^{p-j-1} \sin[\pi(m' + \frac{P}{2})/2^{p-j-1}]} \times \cos \left[\pi \left\{ m' + \frac{k}{2^j} f + \left(1 - \frac{k}{2^j}\right) \frac{P}{2} \right\} / 2^{p-j} \right] \\ &\times \frac{2^{p-j} \sin[\pi(m' + f)/2^{p-j}]}{2^p \sin[\pi(m' + f)/2^p]}. \end{aligned} \quad (\text{B.6})$$

Figure B2 shows a probability distribution of $d_{\text{asc}}^{(e_b)}$, which has a strong peak at $m' = 2^p - f$ and weak peaks near the peak. The second summation in the term $d_{\text{asc}}^{(e_b)}$ also has a strong peak at $m' = f$ and weak peaks near the peak.

Appendix B.1.3. Peaks of the terms $|e_g^{(b)}\rangle$ and $|e_g^{(g)}\rangle$

The terms $|e_g^{(b)}\rangle$ and $|e_g^{(g)}\rangle$, denoted by $|e_g\rangle$, have two summations:

$$\frac{1}{P} \sum_{m=0}^{P-1} e^{\frac{2\pi i}{P}\{mm' + rf\}}, \quad \frac{1}{P} \sum_{m=0}^{P-1} e^{\frac{2\pi i}{P}\{mm' - rf\}}. \quad (\text{B.7})$$

By calculation of summations, we obtain two strong peaks at $m' = f, 2^p - f$ and weak peaks corresponding to the peaks.

Appendix B.1.4. Peaks of all terms

In the case of the ascending-order circuit, all six terms in Equation (B.2) have only two strong peaks at $m' = f, 2^p - f$ that are the same peaks in no error case and weak peaks near two peaks. Hence the overall probability distribution of the quantum state in Equation (B.2) is considered to have two peaks at $m' = f, 2^p - f$.

Appendix B.2. The descending-order circuit

We then investigate probability distributions in the descending-order case. Let r' be the number of controlled- G operations according to the first register $|m\rangle$ before the error.

$$r' := m - 2^j m_j - (m \bmod 2^j) + k m_j.$$

By simple calculation, we obtain the similar final state in Equation (B.2), which uses r' instead of r . We consider peaks of four terms $|e_b^{(b)}\rangle, |e_b^{(g)}\rangle, |e_g^{(b)}\rangle$, and $|e_g^{(g)}\rangle$ in the equation because the terms $|\pm\rangle$ differ little from the case of the ascending-order.

Appendix B.2.1. Peaks of the terms $|e_b^{(b)}\rangle$ and $|e_b^{(g)}\rangle$

Like the ascending-order circuit, the term $|e_b\rangle$ has two summations in this case by replacing r by r' in Equation (B.6). Let $d_{\text{des}}^{(e_b)}$ be the first summation of the term.

$$\begin{aligned} d_{\text{asc}}^{(e_b)} &:= \left| \frac{1}{P} \sum_{m=0}^{P-1} \exp \left[\frac{2\pi i}{P} \left\{ mm' + r'f + (m - r') \frac{P}{2} \right\} \right] \right| \\ &= \frac{\sin[\pi(m' + f)]}{2^{p-j-1} \sin[\pi(m' + f)/2^{p-j-1}]} \times \cos \left[\pi \left\{ m' + \frac{k}{2^j} f + \left(1 - \frac{k}{2^j} \right) \frac{P}{2} \right\} / 2^{p-j} \right] \\ &\quad \times \frac{2^{p-j} \sin[\pi(m' + \frac{P}{2})/2^{p-j}]}{2^p \sin[\pi(m' + \frac{P}{2})/2^p]}. \end{aligned} \quad (\text{B.8})$$

$d_{\text{asc}}^{(e_b)}$ has a strong peak at $m' = -P/2 \equiv 2^p/2$, as shown in Figure B3. This peak corresponds to -1 in the Grover operator in Equation (7). The second summation also has the same peak at $2^p/2$.

Appendix B.2.2. Peaks of the terms $|e_g^{(b)}\rangle$ and $|e_g^{(g)}\rangle$

Let $d_{\text{des}}^{(e_g)}$ be a summation of the term $|e_g\rangle$ corresponding to $d_{\text{asc}}^{(e_g)}$ in Equation (B.7).

$$\begin{aligned} d_{\text{des}}^{(e_g)} &= \frac{\sin[\pi(m' + \frac{P}{2})]}{2^{p-j-1} \sin[\pi(m' + \frac{P}{2})/2^{p-j-1}]} \times \cos \left[\pi \left(m' + \frac{k}{2^j} f \right) / 2^{p-j} \right] \\ &\quad \times \frac{2^{p-j} \sin[\pi m'/2^{p-j}]}{2^p \sin[\pi m'/2^p]}. \end{aligned} \quad (\text{B.9})$$

We show a probability distribution of $d_{\text{des}}^{(e_g)}$ in Figure B4, and obtain a peak at $m' = 0$. The second summation in $|e_g\rangle$ also has the same peak at $m' = 0$.

Appendix B.2.3. Peaks of all terms

The overall probability distribution in the case of the descending-order has four strong peaks at $m' = f, 2^p - f$, i.e. the correct peaks, and $m' = 0, 2^p/2$, particular wrong peaks that do not appear in the ascending-order case and the first register case. The positions of these wrong peaks are fixed independently of an oracle and type of errors.

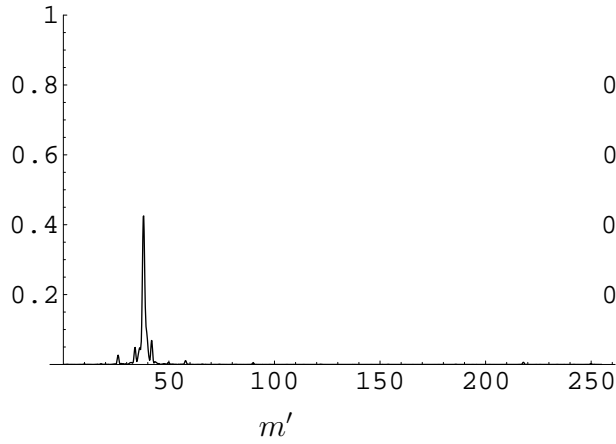


Figure B1. The probability distribution of $d_{\text{asc}}^{(+)}$.

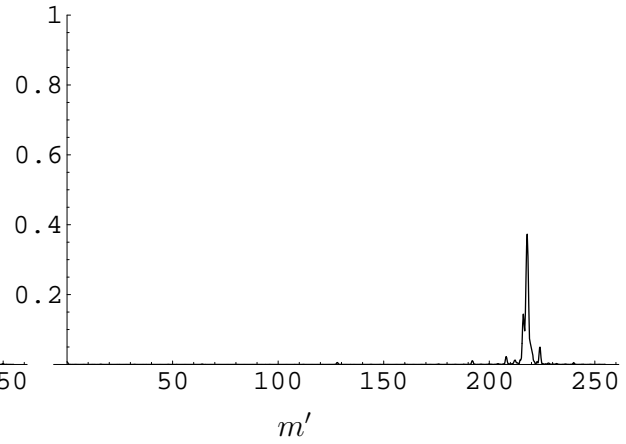


Figure B2. The probability distribution of $d_{\text{asc}}^{(e_b)}$.

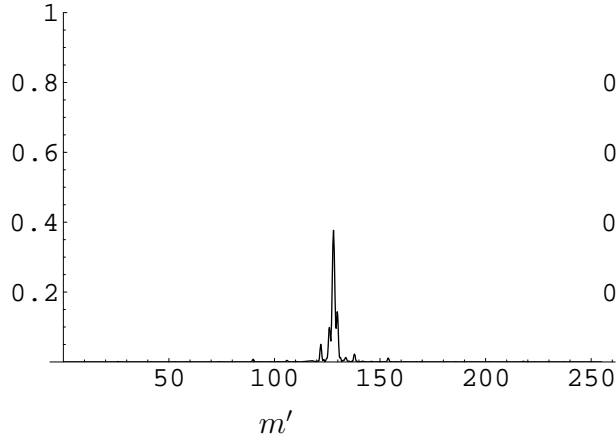


Figure B3. The probability distribution of $d_{\text{des}}^{(e_b)}$.

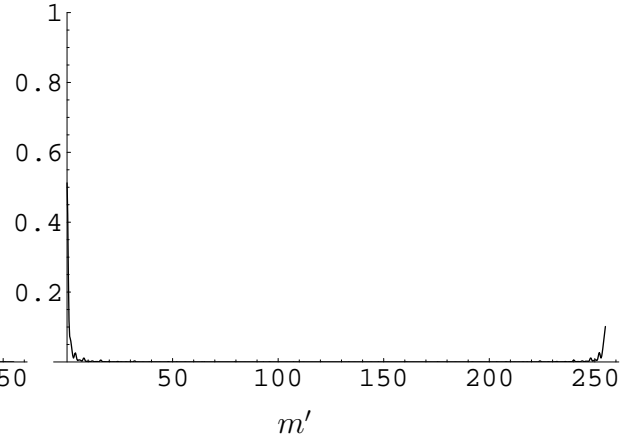


Figure B4. The probability distribution of $d_{\text{des}}^{(e_g)}$.

- [1] D. S. Abrams and C. P. Williams. Fast quantum algorithms for numerical integrals and stochastic processes. arXiv:quant-ph/9908083, 1999.
- [2] H. Azuma. Decoherence in Grover's quantum algorithm: Perturbative approach. *Phys. Rev. A*, **65**(4, 042311), 2002.
- [3] S. Beauregard. Circuit for Shor's algorithm using $2n+3$ qubits, 2002.
- [4] G. Brassard, P. Høyer, and A. Tapp. Quantum counting. In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science*, volume **1443**, pages 820–831, 1998.
- [5] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. arXiv:quant-ph/9607014, 1996.
- [6] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pages 212–219, 1996.
- [7] L. K. Grover. A fast quantum mechanical algorithm for estimating the median. arXiv:quant-ph/9607024, 1996.
- [8] S. Heinrich. Quantum summation with an application to integration. *Journal of Complexity*, **18**:1–50, 2002.

- [9] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University press, 2000.
- [10] J. Niwa, K. Matsumoto, and H. Imai. General-purpose parallel simulator for quantum computing. *Phys. Rev. A*, **66**, 062317, 2002.
- [11] J. Niwa, K. Matsumoto, and H. Imai. Simulating the effects of quantum error-correction schemes. arXiv:quant-ph/0211071, 2002.
- [12] K. M. Obenland and A. M. Despain. Simulating the effect of decoherence and inaccuracies on a quantum computer. *Lecture Notes in Computer Science*, 1509:447–459, 1999.
- [13] S. Parker and M. B. Plenio. Efficient factorization with a single pure qubit and $\log N$ mixed qubits. *Phys. Rev. Lett.*, **14**:3049–3052, 2000.
- [14] D. Shapira, S. Mozes, and O. Biham. Effect of unitary noise on Grover’s quantum search algorithm. *Phys. Rev. A*, **67**(4, 042301), 2003.
- [15] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.
- [16] C.P. Sun, H. Zhan, and X.F. Liu. Decoherence and relevant universality in quantum algorithms via a dynamic theory for quantum measurement. *Phys. Rev. A*, **58**(3), 1998.
- [17] J. F. Traub and H. Woźniakowski. Path integration on a quantum computer. arXiv:quant-ph/0109113, 2002.
- [18] S. Yu and C.P. Sun. Quantum searching’s underlying $SU(2)$ structure and its quantum decoherence effects. arXiv:quant-ph/9903075, 1998.